APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/823,190	03/29/2001	Joseph F. Cihula	42390.P9699	1221

7590   05/27/2005

Jan Carol Little
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER
SALL, EL HADJI MALICK

ART UNIT	PAPER NUMBER
2157	

DATE MAILED: 05/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/823,190	CIHULA, JOSEPH F.
	Examiner	Art Unit	
	El Hadji M. Sall	2157	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 April 2005*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　a)☐ All   b)☐ Some * c)☐ None of:

　　1.☐ Certified copies of the priority documents have been received.

　　2.☐ Certified copies of the priority documents have been received in Application No. _____.

　　3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
　Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
　Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   This action is responsive to the amendment filed on April 26, 2005. Claims 19
and 26-30 are amended. Claims 1-30 are pending. Claims 1-30 represent network-
aware policy deployment.

2.   *Claim Rejections - 35 USC § 102*

       The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that
form the basis for the rejections under this section made in this Office action:
       A person shall be entitled to a patent unless –

       (b) the invention was patented or described in a printed publication in this or a
       foreign country or in public use or on sale in this country, more than one year
       prior to the date of application for patent in the United States.

3.   Claims 1-4, 8, 9, 11, 13-17, 20, 21, 23, and 25-28 are rejected under 35
U.S.C. 102(b) as being anticipated by Raab et al. U.S. 5,751967.

       Raab teaches the invention as claimed including method and apparatus for
automatically configuring a network device to support a virtual network (see abstract).

       As to claim 1, Raab teaches a policy management tool of a system comprising:

dynamic network information (column 6, lines 30-44, Raab discloses the process determines when end-station connectivity changes in the network system, and detects changes to configured policies); and

a policy manager coupled to the model to manage deployment of at least one policy to a set of devices in a network based on the dynamic network information (column 6, lines 38-43, Raab discloses updating devices after changes in the network is detected; column 2, lines 19-22, Raab discloses a configuration policy circuit is provided to reconfigure devices upon modification of the topology).

As to claims 2, Raab teaches the tool of the system of claim 1 wherein the policy manager comprises a policy to restrict certain types of traffic at multiple points within the network via a topology-based analysis of the network (figure 7, item 706; figure 5; column 9, lines 26-30, Raab discloses field 506 in figure 5 specifies whether members matching this policy are allowed as other members specified by the policy (i.e. "restricting certain types of traffic")).

As to claim 3, Raab teaches the tool of the system of claim 1 wherein the policy manager comprises a policy to queue, buffer, or prioritize certain types of traffic at multiple points within the network based on an analysis of traffic found on various portions of the network (figure 7, item 707; figure 5; column 9, lines 36-45, Raab discloses field 507 specifying the priority field indicating the order in which policy entries within the table are evaluated).

As to claim 4, Raab teaches the tool of the system of claims 1 wherein the policy manager comprises a policy to prioritize traffic, wherein the policy automatically selects the prioritization mechanism based on the protocol and/or media the traffic traverses (figure 7, item 707; figure 5; column 9, lines 36-45, Raab discloses field 507 specifying the priority field indicating the order in which policy entries within the table are evaluated).

As to claim 8, Raab teaches the tool of the system of claim 1 wherein the policy manager creates access control lists to control traffic through edge devices in the network based on a topology analysis of the network (column 6,lines 10-20, Raab discloses a network manager (i.e. "the policy manager") may specify that all end-stations having predetermined media access control address within a specified range are member of the same VLAN).

As to claim 9, Raab teaches the tool of the system of claim 1 wherein the dynamic network information comprises a network topology, network statistical information, or network traffic information (column 6, lines 24-27, Raab discloses displaying the physical configuration of the network (topology));

As to claim 11, Raab teaches the tool of the system of claim 1 wherein the policy manager comprises a policy to selectively configure a set of devices based on an analysis of the traffic processed by the set of devices (column 7, lines 43-52, Raab discloses configuration puller 403 generates a list of end-stations requiring evaluation, an this list is passed to a policy evaluation module, which processes each end-station and determine which device need to be reconfigured).

As to claim 13, Raab teaches a method, comprising:
applying dynamic network information to a policy manager (column 6, lines 30-44, Raab discloses the process determines when end-station connectivity changes in the network system, and detects changes to configured policies); and
mapping a policy to a set of devices in the network based on the dynamic network information (column 6, lines 38-43, Raab discloses updating devices after changes in the network is detected; column 2, lines 19-22, Raab discloses a configuration policy circuit is provided to reconfigure devices upon modification of the topology).

As to claim 14, Raab teaches the method of claim 1 wherein the policy manager comprises a policy to restrict certain types of traffic at multiple points within the network via a topology-based analysis of the network (figure 7, item 706; figure 5; column 9, lines 26-30, Raab discloses field 506 in figure 5 specifies whether members matching this policy are allowed as other members specified by the policy (i.e. "restricting certain types of traffic")).

As to claim 15, Raab teaches the method of claim 13 wherein the policy manager comprises a policy to queue, buffer, or prioritize certain types of traffic at multiple points within the network based on an analysis of traffic found on various portions of the network (figure 7, item 707; figure 5; column 9, lines 36-45, Raab discloses field 507 specifying the priority field indicating the order in which policy entries within the table are evaluated).

As to claim 16, Raab teaches the method of claim 13 wherein the policy manager comprises a policy to queue traffic in devices in the network based on priority (figure 7, item 707; figure 5; column 9, lines 36-45, Raab discloses field 507 specifying the priority field indicating the order in which policy entries within the table are evaluated).

As to claim 17, Raab teaches the method of claims 13 wherein the policy manager comprises a policy to prioritize traffic, wherein the policy automatically selects the prioritization mechanism based on the protocol and/or media the traffic traverses (figure 7, item 707; figure 5; column 9, lines 36-45, Raab discloses field 507 specifying the priority field indicating the order in which policy entries within the table are evaluated).

As to claim 20, Raab teaches the tool and the method of claims 1 and 13 wherein the policy manager creates access control lists to control traffic through edge devices in the network based on a topology analysis of the network (column 6,lines 10-20, Raab discloses a network manager (i.e. "the policy manager") may specify that all end-stations having predetermined media access control address within a specified range are member of the same VLAN).

As to claim 21, Raab teaches the tool and the method of claims 1 and 13 wherein the dynamic network information comprises a network topology, network statistical information, or network traffic information (column 6, lines 24-27, Raab discloses displaying the physical configuration of the network (topology));

As to claim 23, Raab teaches the method of claim 13 wherein the policy manager comprises a policy to selectively configure a set of devices based on an analysis of the traffic processed by the set of devices (column 7, lines 43-52, Raab discloses configuration puller 403 generates a list of end-stations requiring evaluation, an this list is passed to a policy evaluation module, which processes each end-station and determine which device need to be reconfigured).

As to claim 16, Raab teaches the method of claim 13 wherein the policy manager comprises a policy to queue traffic in devices in the network based on priority (figure 7, item 707; figure 5; column 9, lines 36-45, Raab discloses field 507 specifying the priority field indicating the order in which policy entries within the table are evaluated).

As to claims 25, Raab teaches an article of manufacture in a system comprising:

Model a topology of a network (column 6, lines 24-27, Raab discloses displaying the physical configuration of the network (topology));

Detect a change in the topology of the network (column 11, lines 43-46, Raab discloses an automatic process which detects changes to the topology);

Apply dynamic network information including the change in the topology of the network to a policy manager (column 6, lines 30-44, Raab discloses the process determines when end-station connectivity changes in the network system, and detects changes to configured policies); and

Map a policy to a set of devices in the network based on the detected change in the topology of the network (column 6, lines 38-43, Raab discloses updating devices after changes in the network is detected; column 2, lines 19-22, Raab discloses a configuration policy circuit is provided to reconfigure devices upon modification of the topology).

As to claim 26, Raab teaches the article of manufacture in the system of claim 25 wherein the policy manager comprises a policy to restrict certain types of traffic at multiple points within the network via a topology-based analysis of the network (figure 7, item 706; figure 5; column 9, lines 26-30, Raab discloses field 506 in figure 5 specifies whether members matching this policy are allowed as other members specified by the policy (i.e. "restricting certain types of traffic")).

As to claim 27, Raab teaches the article of manufacture in the system of claim 25 wherein the policy manager comprises a policy to queue, buffer, or prioritize certain types of traffic at multiple points within the network based on an analysis of traffic found on various portions of the network (figure 7, item 707; figure 5; column 9, lines 36-45, Raab discloses field 507 specifying the priority field indicating the order in which policy entries within the table are evaluated).

As to claim 28, Raab teaches the article of manufacture in the system of claim 25 wherein the policy manager comprises a policy to prioritize traffic, wherein the policy automatically selects the prioritization mechanism based on the protocol and/or media the traffic traverses (figure 7, item 707; figure 5; column 9, lines 36-45, Raab discloses field 507 specifying the priority field indicating the order in which policy entries within the table are evaluated).

4. *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 5, 6, 10, 18, 19, 22, 29 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Raab et al. U.S. 5,751967 in view of Craddock U.S. 6,351,771.

Raab teaches the invention substantially as claimed including method and apparatus for automatically configuring a network device to support a virtual network (see abstract).

As to claims 5, 18 and 29, Raab teaches the tool of the system, the method and the article of manufacture in the system of claims 1, 13 and 25.

Raab fails to teach explicitly a policy to monitor response time of content transfer between one or more primary servers and a device in the network and replicate content of the primary servers to at least one other server when the content time of a primary server exceeds a predetermined metric.

However, Craddock teaches distributed service network system capable of transparently converting data formats and selectively connecting to an appropriate bridge in accordance with clients characteristics identified during preliminary connections. Craddock teaches a policy to monitor response time of content transfer between one or more primary servers and a device in the network and replicate content of the primary servers to at least one other server when the content time of a primary server exceeds a predetermined metric (column 6, lines 5-14, Craddock discloses the determination of whether to replicate the personal agent is based upon a suitable preselected quality of service metric and can include a consideration of the length of the time the user is expected to require access to the data at the local region).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Raab in view of Craddock to provide a policy to monitor response time of content transfer between one or more primary servers and a device in the network and replicate content of the primary servers to at least one other server when the content time of a primary server exceeds a predetermined metric. One would be motivated to do so to provide better performance achievement through distributing file read operations among file system replicas.

As to claims 6, 19 and 30, Raab teaches the tool of the system, the method and the article of manufacture of claims 1, 13 and 25 wherein the policy manager comprises a policy to monitor the performance of one of more servers (column 6, lines 32-35, Raab discloses the virtual auto-configuration monitors the configuration of the network, via examination of topology tables, and determines physical connectivity of VLAN devices).

Raab fails to teach explicitly replicate content of the primary servers to at least one other server when the performance metrics of a primary server exceeds a predetermined value.

However, Craddock teaches replicate content of the primary servers to at least one other server when the performance metrics of a primary server exceeds a predetermined value (column 6, lines 5-14, Craddock discloses the determination of whether to replicate the personal agent is based upon a suitable preselected quality of service metric and can include a consideration of the length of the time the user is expected to require access to the data at the local region).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Raab in view of Craddock to provide the policy manager comprises a policy to monitor the performance of one or more primary servers and replicate content of the primary servers to at least one other server when the performance metrics of a primary server exceeds a predetermined value. One would be motivated to do so to provide better performance achievement through distributing file read operations among file system replicas.

As to claims 10 and 22, Raab teaches the tool of the system and the method of claims 1 and 13.

Raab fails to teach explicitly a policy to replicate content of a first device to a second device when the content response time of the first device exceeds a predetermined metric.

However, Craddock teaches a policy to replicate content of a first device to a second device when the content response time of the first device exceeds a predetermined metric (column 6, lines 5-14, Craddock discloses the determination of whether to replicate the personal agent is based upon a suitable preselected quality of service metric and can include a consideration of the length of the time the user is expected to require access to the data at the local region).

It would have been obvious to one of ordinary skill in the art at the time of the
invention to modify Raab in view of Craddock to create a policy to replicate content of a
first device to a second device when the content response time of the first device
exceeds a predetermined metric. One would be motivated to do so that better
performance can be achieved through distributing file read operations among file
system replicas.

6.   Claims 7, 12 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable
over Raab et al. U.S. 5,751967 in view of Chung et al. U.S. 6,266,781.

Raab teaches the invention substantially as claimed including method and
apparatus for automatically configuring a network device to support a virtual network
(see abstract).

As to claim 7, Raab teaches the tool of the system of claim 1.
Raab fails to teach explicitly the policy manager comprises a policy to monitor the
health of one or more primary servers in the network, to replicate content of the primary
servers to at least one other server when a primary server experiences a fault, and to
configure the other server to emulate the primary server.
However, Chung teaches method and apparatus for providing failure detection
and recovery with predetermined replication style for distributed applications in a
network. Chung teaches a policy to monitor the health of one or more primary servers in
the network, to replicate content of the primary servers to at least one other server when
a primary server experiences a fault, and to configure the other server to emulate the
primary server (column 3, lines 16-29).
It would have been obvious to one of ordinary skill in the art at the time of the
invention to modify Raab in view of Chung to create a policy to monitor the health of one

or more primary servers in the network, to replicate content of the primary servers to at least one other server when a primary server experiences a fault, and to configure the other server to emulate the primary server. One would be motivated to do so to allow each application module running on that host computer is individually failure-protected in accordance with its registered replication style and degree of replication (see abstract).

As to claims 12 and 24, Raab teaches the tool of the system and the method of claims 1 and 13.

Raab fails to teach a policy to replicate content of a first device to a second device when the first device experiences a fault and to configure the second device to emulate the first device.

However, Chung teaches a policy to replicate content of a first device to a second device when the first device experiences a fault and to configure the second device to emulate the first device (column 3, lines 16-29).

It would be obvious to one of ordinary skill in the art at the time of the invention to modify Raab in view of Chung to create a policy to replicate content of a first device to a second device when the first device experiences a fault and to configure the second device to emulate the first device. One would be motivated to do so to allow each application module running on that host computer is individually failure-protected in accordance with its registered replication style and degree of replication (see abstract).

7.   *Response to Arguments*

Applicant's arguments with respect to claim 1-30 have been considered but are moot in view of the new ground(s) of rejection.

8.   ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to El Hadji M Sall whose telephone number is 571-272-4010. The examiner can normally be reached on 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on 571-272-4001. The fax phone number for the organization where this application or proceeding is assigned is 571-273-4010.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

El Hadji Sall
Patent Examiner
Art Unit: 2157
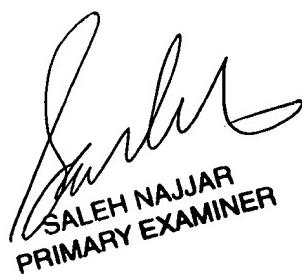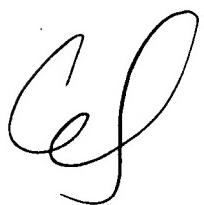
SALEH NAJJAR
PRIMARY EXAMINER